

## CLAIMS

What is claimed is:

- 1 1. A method of producing a uniform duty cycle output from a random bit  
2 source, the method comprising:  
3 testing the duty cycle of the random bit source;  
4 varying the output voltage of a voltage source if the duty cycle is not  
5 substantially fifty percent; and  
6 iteratively altering the output voltage of the voltage source until the duty  
7 cycle is substantially fifty percent.
- 1 2. The method of claim 1 further comprising:  
2 periodically latching a high frequency signal in response to a low  
3 frequency signal; and  
4 outputting one or more binary digits corresponding to a voltage level of  
5 the latching high frequency signal.
- 1 3. The method of claim 1 wherein varying the output voltage of the voltage  
2 circuit further comprises updating the threshold voltage of a flash memory cell in  
3 the voltage circuit.
- 1 4. The method of claim 1 wherein varying the output voltage of the voltage  
2 circuit further comprises:  
3 varying an input current to a non-inverting input of a differential  
4 amplifier to produce a first input voltage; and

5           varying an input current to an inverting input of the differential amplifier  
6   to produce a second input voltage.

1   5.     The method of claim 1 wherein varying the output voltage of the voltage  
2   circuit further comprises altering the number of transistors in the voltage circuit  
3   determining the output voltage.

1   6.     The method of claim 1 wherein the method of producing a uniform duty  
2   cycle output from a random bit source is used in a random number generator  
3   operable to produce random binary numbers for use in a cryptographic system  
4   for secure communications between a plurality of computers in a network.

1   7.     A programmable random bit source comprising:  
2         a latch having a data input and a clock input;  
3         a first oscillator coupled to the data input of the latch, the first oscillator to  
4   output a first oscillating signal; and  
5         a second oscillator coupled to the clock input of the latch circuit, the  
6   second oscillator to output a second oscillating signal having a frequency slower  
7   than a frequency of the first oscillating signal.

1   8.     The programmable random bit source of claim 7 further comprising a  
2   programmable voltage source coupled to a bias input of the latch.

1   9.     The programmable random bit source of claim 8 wherein the  
2   programmable voltage source comprises:  
3         a first flash memory cell;  
4         a second flash memory cell; and

5 a differential amplifier having a first input coupled to the first flash  
6 memory cell, and a second input coupled to the second flash memory cell.

1 10. The programmable random bit source of claim 7 wherein the  
2 programmable voltage source comprises:  
3 a first resistor;  
4 a second resistor; and  
5 a differential amplifier having a first input coupled to the first resistor,  
6 and a second input coupled to the second resistor.

1 11. The programmable random bit source of claim 7 wherein the  
2 programmable voltage source comprises a logic gate having:  
3 a first pull-up transistor;  
4 a first pull-down transistor; and  
5 a second pull-up transistor coupled in parallel with the first pull-up  
6 transistor.

1 12. The programmable random bit source of claim 11 wherein the logic gate  
2 further comprises means for selectively enabling the second pull-up transistor.

1 13. The programmable random bit source of claim 7 wherein the  
2 programmable voltage source comprises a logic gate having:  
3 a first pull-up transistor;  
4 a first pull-down transistor; and  
5 a second pull-down transistor coupled in parallel with the first pull-down  
6 transistor.

1 14. The programmable random bit source of claim 13 wherein the logic gate  
2 further comprises means for selectively enabling the second pull-down  
3 transistor.

1 15. The programmable random bit source of claim 7 wherein the latch has an  
2 adjustable trip point.

1 16. The programmable random bit source of claim 15 further comprising a  
2 programmable voltage source coupled to a bias input of the latch, wherein the  
3 adjustable trip point of the latch is alterable by a voltage output by the  
4 programmable voltage source.

1 17. A programmable random bit source comprising:  
2 a latch having a data input and a bias input;  
3 a programmable voltage source coupled to the bias input of the latch;  
4 a comparator having an output coupled to the data input of the latch;  
5 a resistor-inductor-capacitor circuit coupled to an input of the comparator;  
6 and  
7 a noise source coupled to the resistor-inductor-capacitor circuit.

1 18. The programmable random bit source of claim 17 wherein the latch has an  
2 alterable trip point.

1 19. A digital processing system comprising:  
2 an encryption/decryption circuit comprising a random number generator  
3 having,  
4 a latch having a data input and a clock input;

5                   a first oscillator coupled to the data input of the latch, the first  
6 oscillator to output a first oscillating signal; and  
7                   a second oscillator coupled to the clock input of the latch circuit, the  
8 second oscillator to output a second oscillating signal having a frequency  
9 slower than a frequency of the first oscillating signal.

1   20.    The digital processing system of claim 19 wherein the programmable bit  
2 source further includes a programmable voltage source coupled to a bias input of  
3 the latch.

1   21.    The digital processing system of claim 20 wherein the latch has an  
2 adjustable trip point, wherein the adjustable trip point of the latch is alterable by  
3 a voltage output by the programmable voltage source.

1   22.    The digital processing system of claim 19 wherein the  
2 encryption/decryption circuit to encode and decode messages transmitted and  
3 received by the digital processing system using a cipher-based cryptographic  
4 method.

1   23.    The digital processing system of claim 22 wherein the cipher-based  
2 cryptographic method is a single key system.

1   24.    The digital processing system of claim 22 wherein the cipher-based  
2 cryptographic method is a public key/private key system.